UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,689	10/17/2003	James M. Doherty	1033-T00534C	2688

60533 7590 08/06/2008

TOLER LAW GROUP
8500 BLUFFSTONE COVE
SUITE A201
AUSTIN, TX 78759

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/605,689	DOHERTY ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-16 and 18-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-16 and 18-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on May 02, 2008.

2. Claims 1-2, 4-16 and 18-25 have been examined and are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-2, 4-16 and 18-25 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2, 4-16 and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moran (US Pat. No.: 6, 647, 400) in view of Rowland et al. (hereinafter referred to as Rowland, US Pub. No.: 2002/0129264).

As per claim 1:

Moran discloses an method for detecting intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, the method comprising:

monitoring data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database (column 4: lines 1-15; figure 9: compute signature of a file; Does signature match the previously computed signature for file; Abstract; column 4: lines 17-23; column 32: lines 49-59).

Moran does not explicitly disclose upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host and issuing a command to an operating system of said host to bring said host to a single user state. Rowland, in analogous art, however, discloses upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host and issuing a command to an operating system of said host to bring said host to a single user state (0037; 0053; 0065; 00145; 0148). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include and issuing a command to an operating system of said host to bring said host to a single user state. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a generic distributed command, control, and communication framework that allows

computer systems, devices, and operational personnel to interact with a network as a unified entity as suggested by Rowland (0007).

As per claim 2:

Rowland discloses issuing a command to bring down said one or more network interfaces to isolate and host upon identifying the mismatch in compared digital signatures (0037; 0053; 0065; 00145; 0148)..

As per claim 4:

Rowland discloses said first remote database and said second remote database are located on a single server or a plurality of servers belonging to a local area network (0037; 0053; 0147).

As per claim 5:

Rowland discloses communications between said host and first remote database are encrypted (0027; 0068; 0074; 075).

As per claim 6:

Rowland discloses communications between said host and second remote database are encrypted (0027; 0068; 0074; 075).

As per claim 7:

Moran discloses said digital signature is an MD5 signature and said first remote database is an MD5 database (column 31: lines 46-55).

As per claim 8:

Moran discloses said second remote database is a SYSLOG database (column 24: lines 47-64).

As per claim 9:

Moran discloses said data entities comprises one or more system files, configuration files, or directories (column 4: lines 5-35).

As per claim 10:

Moran discloses a system to detect intrusion comprising:

a host running a monitoring daemon working in conjunction with a configuration file, said configuration file identifying files and directories to be monitored in said host and said host communicating with external networks via one or more network interfaces, said monitoring daemon dynamically monitoring said files and directories identified by said configuration file by comparing a locally stored digital signature corresponding to each file or directory against a remotely stored corresponding digital signature (column 4: lines 1-15; figure 9: compute signature of a file; Does signature match the previously computed signature for file);

a digital signature database remote from said host storing said digital signatures associated with files and directories identified by said configuration file (Abstract; column 4: lines 17-23; column 32: lines 49-59); and

a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database (column 32: lines 6-22; column 32: lines 49-59; column 33: lines 36-41).

Moran does not explicitly disclose a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database and wherein a mismatch identifies a possible intrusion in the host, resulting in a command being issued to an operating system of said host to bring said host to a single user state. Rowland, in analogous art, however, discloses a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database and wherein a mismatch identifies a possible intrusion in the host, resulting in a command being issued to an operating system of said host to bring said host to a single user state (0037; 0053; 0065; 00145; 0148). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include a log database remote from said host recording entries corresponding to mismatches between a digital signature stored in said host and a corresponding digital signature in said digital signature database and wherein a mismatch identifies a possible intrusion in the

host, resulting in a command being issued to an operating system of said host to bring said host to a single user state. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a generic distributed command, control, and communication framework that allows computer systems, devices, and operational personnel to interact with a network as a unified entity as suggested by Rowland (0007).

As per claim 11:

Moran discloses a system to detect intrusion, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network (figure 3: 306, 308, 304).

As per claim 12:

Rowland discloses a system to detect intrusion, wherein communications between said host and said digital signature database are encrypted (0027; 0068; 0074; 075).

As per claim 13:

Rowland discloses a system to detect intrusion, wherein communications between said host and log database are encrypted (0027; 0068; 0074; 075).

As per claim 14:

Moran discloses a system to detect intrusion, wherein said digital signature is an MD5 signature and said first remote database is an MD5 database (column 31: lines 46-55).

As per claim 15:

Moran discloses an article of manufacture comprising a computer usable medium having computer readable program code embedded therein to detect intrusion in a host via a monitoring daemon operating in conjunction with a configuration file defining data entities to be monitored, said medium comprising:

computer readable program code comprising executable instructions to monitor data entities via comparing a locally stored copy of a digital signature associated with each data entity against a corresponding digital signature stored in a first remote database (column 4: lines 1-15; figure 9: compute signature of a file; Does signature match the previously computed signature for file; Abstract; column 4: lines 17-23; column 32: lines 49-59);

Moran does not explicitly disclose computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host and computer readable program code. comprising executable instructions to issue a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures. Rowland, in analogous art, however, discloses computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote

database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host and computer readable program code. comprising executable instructions to issue a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures (0037; 0053; 0065; 00145; 0148). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include computer readable program code comprising executable instructions to issue an instruction to record an entry in a log file located in a second remote database upon identifying a mismatch in compared digital signature, said entry identifying a possible intrusion in said host. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a generic distributed command, control, and communication framework that allows computer systems, devices, and operational personnel to interact with a network as a unified entity as suggested by Rowland (0007).

As per claim 16:

Rowland discloses an article of manufacture, further comprising computer readable program code comprising executable instructions to issue a command to bring down one or more network interfaces to isolate said host upon identifying the mismatch in compared digital signatures (0037; 0053; 0065; 00145; 0148)..

As per claim 18:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, said host having one or more network interfaces to communicate over one or more networks, said method comprising:

reading a configuration file to identify data entities to be monitored on a host (column 4: lines 1-15);

for each data entity to be monitored, extracting a digital signature from said host (figure 9: compute signature of a file);

for each data entity to be monitored, querying a remote digital signature database via said one or more network interfaces and requesting a digital signature corresponding to said digital signature extracted from said host (figure 9: Does signature match the previously computed signature for file);

for each data entity to be monitored, receiving said corresponding digital signature from said remote digital signature database (figure 3: 308, 306, 304, 312); and

matching digital signature received from said remote digital signature database with digital signature extracted at said host (Abstract; column 4: lines 17-23; column 32: lines 49-59).

Moran does not explicitly disclose upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host and issuing a command to an operating system of said host to bring said

host to a single user state. Rowland, in analogous art, however, discloses upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host and issuing a command to an operating system of said host to bring said host to a single user state (0037; 0053; 0065; 00145; 0148). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Moran to include upon identifying a mismatch, transmitting an instruction to a remote log database via said one or more network interfaces, said instruction executed in said remote log database to record an entry in a log file indicating a possible intrusion in said host and issuing a command to an operating system of said host to bring said host to a single user state. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a generic distributed command, control, and communication framework that allows computer systems, devices, and operational personnel to interact with a network as a unified entity as suggested by Rowland (0007).

As per claim 19:

Rowland discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said digital signature database and said log database are located on a single server or a plurality of servers belonging to a local area network (0037; 0053; 0147).

As per claim 20:

Rowland discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein communications between said host and digital signature database are encrypted (0027; 0068; 0074; 075).

As per claim 21:

Rowland discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein communications between said host and log database are encrypted (0027; 0068; 0074; 075).

As per claim 22:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said digital signature database is an MD5 database (column 31: lines 46-55).

As per claim 23:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said log database is a SYSLOG database (column 24: lines 47-64).

As per claim 24:

Moran discloses an intrusion detection and isolation method implemented using a monitoring daemon in a host, wherein said data entities are any of the following: system files, configuration files, or directories (column 4: lines 5-35).

As per claim 25:

Rowland discloses the intrusion detection and isolation, further comprising issuing a command to bring down said one or more network interfaces to isolate said host (0037; 0053; 0065; 00145; 0148)..

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136